Configure Common Security Settings

Introduction to Exercise

As an admin, there are some basic security settings you can enable and adjust in the Admin console to improve the overall security of your Cloud Identity instance.

Exercise Scenario

In this exercise, you'll modify and enable security features and settings for your entire domain.

Exercise Directions

1. Sign into your Google Admin console as the administrator user with **your administrator account name and password**.

2. From the **Admin console dashboard,** click on the **Security icon**.

3. Click on **Basic settings** to ensure **security features and settings are enabled** in the following sections:

- Password Recovery
- 2-step verification
- Less secure apps

4. By default, only a domain administrator can reset a user's password. The **Password Recovery** setting is applicable where you want to allow users to recover their own passwords. This achieved through the use of a recovery email address or phone number. To enable user password recovery, click the **Enable/disable non-admin user password recovery link**, and check **Enable non-admin user password recovery**.

Note:

- *See Set up password recovery for users for details on how to let your users reset their own passwords.*

5. In the **2-Step Verification section**, check **Allow users to turn on 2-step verification**.

- This makes 2-Step Verification available for your users, but does not automatically enroll them. To enroll, users need to configure their verification settings individually.
- Once all users have enrolled in 2-Step Verification, you can enforce 2-step verification.

Note:

- *See Set up 2-Step Verification for your domain for more information on how to enable 2-Step Verification, account recovery recommendations, and tips for deploying to your users.*

6. In **Less secure apps**, you can control access **to third-party apps that use less secure sign-in technology**. You can choose to deny access for these apps, which we recommend, or choose to allow access despite the risks.

- Click on the link **Go to settings for less secure apps >>**. In the window that opens, your list of organizational units will be displayed in the left sidebar.
- **Click on the organizational unit to which you wish to apply the setting**.

Note:

- *By default, the box to Allow users to manage their access to less secure apps is checked.*
- *See Control access to less secure apps.*

7. Expand the **Password management** section. This is where password policies are set.

You can enforce strong passwords by checking the **Enforce strong password** box. You can also set a **Password length** policy by setting minimum and maximum length values. It is recommended to keep the minimum password length to at least 8 characters. You can enforce the length and strength policies when your users next login to their account or when they next change their password. The default enforcement is when the password is next changed.

The **Allow password reuse** box allows you to control whether your users can reuse their old passwords. We recommend you leave this option unchecked to prevent reuse.

You can also force your users to change their passwords after a certain number of days or allow them to never expire with the **Password expiration** setting. We recommend you allow passwords to never expire.

Note:

- *See Manage your users' password settings for more information on how to help keep your user's account secure.*

- *See Create a strong password & a more secure account for more information on how to choose a strong password.*

8. In **API reference**, check **Enable API access** to enable programmatic access to your Cloud Identity domain.

Note:

- *You have access to the Admin SDK—a collection of Application Programming Interfaces (APIs), so you can build customized administrative tools for your Google products. Before you can use the Admin SDK, you need to enable API access.*
- *See Enable API access in the Admin console*

9. In **Set up single sign-on (SSO)**, you can enable your users access to many applications without having to enter their username and password for each application.

- In the Setup SSO with Google identity provider option, you can set up SSO using Google as the identity provider using Security Assertion Markup Language (SAML), the user can use their managed Google account credentials to sign in to enterprise cloud applications.
- In the Setup SSO with third party identity provider option, you can set up SSO using a third-party as the identity providers so that Google is the service provider and users authenticate through a third-party Identity provider.

Congratulations! You can now view and modify basic security settings for your entire domain.

Revision #1
Created 2026-02-10 01:19:21 UTC by joliveira
Updated 2026-02-10 01:19:42 UTC by joliveira